REQUEST FOR PROPOSAL

January 21, 2022

FINCA MICROFINANCE BANK LIMITED

FINCA House, 36/B Sector XX, Main Khayaban-e-Iqbal, DHA Phase III Lahore.

Contents

Contracting Party

FINCA Microfinance Bank Limited

Introduction

Fraud can generally be defined as criminal deception intended to result in financial or personal gain. Fraud encompasses a variety of crimes that include, but are not limited to; fraud by false representation, fraud by failing to disclose information, fraud by abuse of position and obtaining services dishonestly. Fraud is one of the top threats to financial institutions (FIs) and their customers. An identity theft crime, account takeover comes in many different forms. Fraudsters have a variety of weapons and methods of harvesting personal data and causing serious damage, which makes effective protection a challenge. The right multi-layered security approach, however, can help block account takeover fraud and protect customers at every stage of their digital journeys. Fraud Risk Management System is a best practices approach to deducting and preventing the fraud with supported technologies that protect users, system/device and transactions of the bank.

Objective

The challenge with transaction monitoring is finding the right balance between achieving regulatory compliance and minimizing the administrative impact on the business, while at the same time, limiting the number of false alerts. This requires a risk based approach that is customized to the business nature, product range, transaction types, regions of activity, etc.

There is a need for a modular and complete Anti-Fraud Management system that provides alerts on real-time basis as well as allowing Bank to detect suspicious activities on early stages preventing to become of fraudulent nature.

FMBL's vision is to establish a safe & secure payment infrastructure and ecosystem which would act as the central hub of mobile & card driven payments and bring benefits to financial institutions / individuals that in aggregate impact the economy and society by significantly increasing access to formal financial services.

Purpose of this RFP

Due to the increasing volume of transactions, it is ever more difficult to identify fraud by conventional methods and via data analysis. At the same time, it is no longer reasonable to expect that end-users will be able to defend themselves against more and more sophisticated types of fraud attempts with growth in technology and Alternate Delivery Channels involvement in day to day banking needs. And in most cases, providers of financial services are responsible for fraud damages, which increases the cost of doing business. Due to this FINCA Microfinance Bank Ltd. requires an anti-fraud management system to conduct online channel monitoring on 24/7 basis covering all channels i.e. Mobile Application (Mobiliser), Debit

Cards (ON-US), Online transactions, Core Banking Transactions (AB-III) and other digital channel transactions as well.

In addition to this there is also a need to have additional, non-interfering level of protection for end users as well as automatic data gathering and analysis to mitigate the risks of traditional, online and card skimming frauds.

Scope of our Work

1. General Requirement

FINCA Pakistan is looking for Fraud Risk Management solution providing end to end facility to detect & prevent fraudulent activities on cards (ATM, POS), E-commerce, SIMSIM App, Core Banking System. Basically this system shall serve as a host, generating alerts as well as preventing suspicious activities in different phases whereby under phase 'I' bidder shall be able to provide ON-US (all transactions being executed on FINCA's own network) module **before 31-Mar-22** and through Phase 'II' it shall cover Preventive module covering Branch and Branchless Banking transactions. The system shall provide 24/7 services without having any unnecessary intervals-gap/ uninformed system up-grading.

SBP's requirement of PSD circular no. 9 of 2018

"All card issuing/acquiring banks/MFBs shall deploy real-time fraud monitoring tools and alert mechanisms, preferably provided by their Payment Schemes, to detect potential fraudulent activities on their Card Systems latest by January 31, 2019.

Banks/MFBs shall make arrangements to monitor on 24/7 basis usage/activity regarding payments made through their cards or through online transactions on their internet banking platforms."

2. Primary Requirement

- The proposed solution shall comply with various regulatory body policy and other industry-based standards related to electronic payments and it shall have good reputation as well as satisfy all requirement criteria
- The solution shall allow FINCA Pakistan to configure its own rules within the Anti-Fraud Management System without dependency on vendors at no extra cost
- The proposed solution shall identify & prevent fraudulent transactions which are linked to a non-monetary transaction such as mobile number/device change, ATM PIN change, any static data change such as name, signature and picture, address, balance enquiry, etc.
- The proposed solution shall provide the capability to detect, discover, prevent and alert the frauds in real-time not only restricted to one channel but across all the channels mentioned i.e. Core Banking System, Mobile Banking, E-commerce, ATM, Mobile Wallets, Debit Card & POS
- The system shall generate different levels of dashboards and Management Information System (MIS) Reports to meet the requirements of individual user/ management level/ all demographic level

- The proposed solution shall integrate with automated IVR & SMS based alert facility on 24X7 basis to confirm with a customer in case of high-risk transactions
- The proposed solution shall provide 'Advanced Machine Learning (AI)' based predictive scoring capabilities
- The proposed solution shall provide a web-based scenario authoring tool to configure new fraud schemes as and when required
- The Fraud Detection & Prevention solution shall provide open APIs so that the Bank's different applications can be integrated with the Fraud Detection & Prevention solution
- The proposed solution shall provide complete evidence for why a transaction was declined/ hold by the fraud management system
- The proposed solution shall provide a complete audit trail
- The proposed solution shall support built-in maker checker functionality to ensure dual commit to critical system changes.
- The proposed solution shall provide MIS dashboard and reports for tracking fraud cases, users performance and system performance.
- The Fraud Detection & Preventions solution/software developed or customized shall follow a standard development process to ensure that it meets the functional, security, performance & regulatory requirements of the Bank.
- The vendor shall provide implementation plan, manual, technical specification document and trainings all inclusive
- Comparing amounts and frequencies to known fraud trends and parameters
- Allowing authorized employees to create reports based on selected criteria
- Detecting suspicious activity based on customers' previous activity
- System will not split to acquirer and issuer functionalities; it is oriented to detect fraud in the whole chain from point of sale to card members
- Highly efficient rule processing engine
- Mandatory Daily Transaction Monitoring Parameters
- FRMS shall provide the tools and information to identify, investigate, and track workflow in response to incident/ case management
- System should be capable to swift integration with the Bank systems & infrastructure in the light of PCI-DSS & PA-DSS guidelines together with EMV standards
- FRMS System shall work proactively to detect and prevent battle against fraud in order to:
    - Reduce risk of fraud and fraudulent activities
    - Detect fraudulent activity
    - Reduce opportunities to commit fraud

3. Mandatory Requirements

- System shall detect suspicious patterns based upon alert generated data using advanced analytical tools, and deliver the information to the user in form of Dashboard
- System shall have the capability to analyze large data volumes with speed & accuracy, and deliver the information to end user

- System shall have the functionality to generate alerts for cash deposits, withdrawals, Internal and External Funds Transfers from multiple location within same & cross city within specified timeframe
- System shall detect geo-location (lat/long) and provide representation of fraudulent behavior of cash withdrawal & deposit and provide the details to user end
- System will be capable to monitor the online behavior of the customers with various transactional patterns fed by the bank's team
- Perform real-time checking of all Branch & Branchless Banking, Debit Cards & Mobile Banking transactions instigated from the listed platforms
- Generate reports to enable bank gauge analyst effectiveness and rule performance.
- Ease of rule creation and deployment in real time
- Ability to trigger alerts in real time environment
- System should be capable of defining rules as required by "International Standards" for Issuing & Acquiring businesses for ATM/Debit Cards and transactions performed through different channels
- System should have standard audit and performance log/reports and should also support customized reports
- Ability to detect/identify point of compromise
- Rule queuing & rule prioritizing agent wise/nature of transaction wise/Portfolio wise
- System should be able to allow users to forward/assign rules to other users also to set reminders on any rule which requires action in later stages
- System should be able to generate alerts via email in case action on any of the triggered/ fired rule is not taken by the user in specified time period in system
- System should be able to allow users to mark fraud on individual transactions
- Ability to search any individual transaction by "Account Number" by "Agent/Merchant Name" by "Device Number" by "Transaction ID" by "Token Number" by "Account handler CNIC" and by "Debit Card Number"
- Ability to do external linking into the system for monitoring purpose
- Ability to prioritize and organize the workflow of alerts for review and measuring the performance and efficiency of the analyst

4. Key Functions Requirement

Detect a wider range of Fraud by combining machine learning with an advanced rule engine. For example, the rule engine will catch transactions where time, place or amount values deviate from a normal scenario. It can also help with detecting more sophisticated cases, like skimming, phishing attacks or transactions to mule accounts.

Quotation

Interested firms may send the quotations till February 4, 2022 working days. The firms are required to include the following information in their proposal, as a minimum:

- Experience of undertaking similar projects for multinationals or large local organizations

- Declaration and Work order copies to be submitted
- Declaration or statement/ confirmation letter that compatibility issues will be avoided and will not take place
- Copy of confirmation letter from Financial Institution(s) with which delivery channel interface has been done
- Detailed methodology to be adapted
- Profile of the key members to be involved in the project and their exposure
- Project cost including all applicable taxes. Cost must be in PKR.
- Project timeline
- Deliverables

Selection & Evaluation Criteria

1. Selection Criteria

Firm for the captioned assignments shall be selected based on the following criteria;

- Have prior experience of working on similar projects of multinationals or large local organizations.
- Be a member Pakistan Software Houses Association (PASHA) or Pakistan Software Export Board (PSEB) or leading international software development and implementation company in financial sector.
- Not blacklisted by reputable multinationals or large local organization on basis of non-performance
- Registered with FBR for taxation purposes

2. Evaluation Criteria

Firm evaluation scoring shall be as under:

Description	**%age**
Technical	30%
Be a member Pakistan Software Houses Association (PASHA) or Pakistan Software Export Board (PSEB) or leading international software development and implementation company in financial sector	20%
Qualification & experience of personnel that will be deployed on this project	20%
Number of similar assignments recently completed for large Organizations / multinationals	30%

General Terms and Conditions

- All documents and reports submitted by the firms shall be the property of FINCA
- The firm shall not re-assign the work to any other firm/ entity
- All costs related to assignments preparation and submission will be borne by the firm
- The firm will be required to sign a confidentiality (Non-disclosure) agreement before the contract is awarded

- FINCA Pakistan reserves the right to;
  - Reject or accept any quotation from any party
  - Not respond to a request made by any party. The proposal submitted shall not be construed as or intended to be an offer

Contact Details

Following persons can be contacted in case of any questions.

Department	Compliance & Internal Controls	Admin & Procurement Department
Name	Mr. Zeeshan Muhammad Sharif	Mr. Mohsin Jamil Ahmed
Designation	Unit Head AML CFT & Regulatory	Sr. Manager Procurement
Cell no.	+92 042 3666 7903 (Ext. 323)	+92 042 3666 7903 (Ext. 214)
Email	zeeshan.muhammad@finca.pk or frmu@finca.pk	mohsin.jamil@finca.pk
Address	FINCA House 36-B, XX Phase III Khayaban-e-Iqbal DHA Lahore	FINCA House 36-B, XX Phase III Khayaban-e-Iqbal DHA Lahore